UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF VERMONT

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 2:16-cr-154
	)	
JAMES COYNE,	)	
Defendant.	)	

OPPOSITION TO MOTION TO SUPPRESS EVIDENCE AND STATEMENTS

The United States of America, by and through its attorney, Eugenia A. P. Cowles, Acting United States Attorney for the District of Vermont, respectfully submits this memorandum in opposition to Coyne's Motion to Suppress, filed May 17, 2017.

I. INTRODUCTION

The Motion proceeds from several faulty premises. First, it omits or obscures a crucial fact featured prominently in the complaint affidavit and other discovery, namely, that, unlike in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), the Electronic Service Provider (ESP) here, Microsoft, examined the child pornography transmissions in question before forwarding them to the National Center for Missing and Exploited Children (NCMEC). Next, it relies wholly on *Ackerman*, without so much as alluding to the landscape of cases that finds no Fourth Amendment violation where an ESP is first reviewer. It also skirts around *Ackerman's* acknowledgement that it might well have found no Fourth Amendment violation had (1) the lower court made adequate factual findings concerning the "third party doctrine," and (2) the ESP reviewed all of the material in question, thereby triggering the "private search doctrine."

To begin, *Ackerman*, which deemed NCMEC a government entity, was wrongly decided under controlling Supreme Court and Second Circuit case law. In any event, here, because private entity Microsoft reviewed Coyne's contraband transmissions, the search did not run afoul

of the Fourth Amendment. Moreover, because Coyne, in signing up for an account, agreed to allow Microsoft to seize his content, the "third party doctrine" also presents an insurmountable barrier to his Motion. Finally, aside from misapprehending or ignoring essential facts and relying myopically and inaptly on *Ackerman*, the Motion has no answers for the good faith doctrine. Even if there was a Fourth Amendment violation – and there was not – the good faith exception undoubtedly precludes application of the exclusionary rule in this case.

For these and other reasons outlined below, the Court should deny the Motion.

II. FACTUAL BACKGROUND

A. Microsoft

Microsoft Corporation owns Skype, an online application that facilitates communication in various forms, including through instant messaging and the sharing of files through instant messaging. Microsoft is an ESP and "professional entity" within the meaning of 18 U.S.C. § 2258. That statute provides, in pertinent part: "A person who, while engaged in a professional capacity . . . . learns of facts that give reason to suspect that a child has suffered an incident of child abuse . . . . and fails to make a timely report . . . . shall be fined under this title or imprisoned not more than 1 year or both." *Id.* Upon learning of such facts, the ESP must report the matter to NCMEC's CyberTipline, including details about user identifying information, geographic location, and any images of apparent child pornography connected to the user. *Id.* § 2258A(b). The statutory scheme does *not* require ESPs to act affirmatively to monitor user accounts, review their communications or uploads/downloads, search for child pornography, or maintain any sort of reporting system for abuse of the ESP's services. *Id.* §§ 2258, 2258A. In fact, the statute specifically states that it does not impose such requirements: "[n]othing in this section shall be construed to require an electronic communication service provider . . . to – (1) monitor any user, subscriber, or customer of that provider; (2) monitor the content of any

communication of any person described in paragraph (1); or (3) affirmatively seek facts or circumstances described in sections (a) and (b)." 18 U.S.C. § 2258A(f).

Microsoft has long viewed a safe online environment as a key selling point for its products and services. *See* Exhibit 1, Affidavit of Microsoft Corporation Chief Online Safety Officer, Jacqueline F. Beauchere, in Support of Order to Show Cause to Quash Subpoena, dated January 30, 2015, filed in *People v. Price*, No. 1106-14, Suffolk County, New York, ¶ 2.[1] As a result, Microsoft employs "family safety technology tools," which are not legally required, but valued by its customers. In addition, the company provides online resources to promote personal and family online safety. In the same vein, Microsoft requires users to agree to a "Code of Conduct" that sets online community standards (described in greater detail below). *Id.* ¶ 3.

PhotoDNA technology is a component of Microsoft's voluntary business strategy to create a safe online environment. PhotoDNA is an image-matching technology developed by Microsoft in collaboration with Dartmouth College that helps Microsoft find and remove images of child sexual abuse from its online services. *Id.* ¶ 4. The technology relies on a mathematical algorithm to create a unique signature – similar to a fingerprint – for each digital image. Once PhotoDNA generates a unique digital signature, it can be compared with signatures of other images to find copies of the image or the original. *Id.* ¶ 7 (describing process in detail). The technique is commonly known as "hashing," but PhotoDNA's hashing system is more robust and reliable than other hashing technologies. *Id.* ¶ 8. Microsoft uses PhotoDNA on several of its services, including Skype. Exhibit 2, Declaration of Jeff Lilleskare, group manager for security and online safety at Microsoft Corporation, dated 6/21/17, ¶ 2.

[1] Microsoft asked the government to rely on this Affidavit for the relevant generic information. Microsoft provided a separate Declaration that addresses the specific facts of this case.

"Microsoft developed and implemented PhotoDNA as a result of its independent judgement that blocking illegal images of child sexual abuse from its services is in Microsoft's business interests." *Id.* ¶ 5 (detailing the "direct and indirect costs" of having such images on its services, including consumer complaints and harm to marketplace image and reputation). "No government agency or law enforcement officer directed or requested that Microsoft create or use PhotoDNA." *Id.* ¶ 6.

If the hash value of PhotoDNA-scanned content matches the hash value of a known image of child sexual abuse (a "hit"), Microsoft takes several steps to prevent the continued access to and/or transmission of the images, to protect its customers, and to report the images as required by law. First, it suspends the account and, with it, the customer's access to it or any associated account. Next, as required by federal law, it files a CyberTipline report with NCMEC, which contains information such as the name of the "hit" file, the associated IP address, and the name and email address provided in connection with the account registration. *Id.* ¶ 10.

Microsoft's Services Agreement is available online; its most recent iterations are attached to Exhibit 2. *See* Exhibit 2, Attachment B; *see also* https://www.microsoft.com/en-us/servicesagreement/.[2] The Agreement covers the Skype service. Exhibit 2, Attachment B, at 810. In the preamble, the Agreement states: "You accept these Terms by creating a Microsoft account or Skype account, through your use of the Services, or by continuing to use the Services after being notified of a change to these Terms." *Id.* Under the heading, "Your Privacy," the Agreement provides: "By using the Services or agreeing to these Terms, you consent to

[2] In the government's view, the version that went into effect on August 1, 2015 applies to the conduct in this case, which occurred in May through August, 2016. Accordingly, this brief will cite to that iteration of the Agreement.

Microsoft's collection, use and disclosure of Your Content and Data as described in the Privacy Statement." The Privacy Statement (embedded by hyperlink in the online version) explains "what personal data we collect from you and how we use it." Exhibit 2, Attachment B, at 871; *see* also https://privacy.microsoft.com/en-us/privacystatement. It further explains:

> We collect content of your files and communications when necessary to provide you with the products you use. . . . Examples of this data include: the content of your documents, photos, music, or videos you upload to a Microsoft service such as OneDrive, as well as the content of your communications sent or received using Microsoft products such Outlook.com or Skype, including the:
>
> •subject line and body of an email,
>
> •text or other content of an instant message,
>
> •audio and video recording of a video message, and
>
> •audio recording and transcript of a voice message you receive or a text message you dictate.

Id. at 871-72.

The Privacy Statement also provides an explanation of the reasons Microsoft shares data. It provides, in part:

> [W]e will access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to:
>
> 1. comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies . . . .

Id.

The Services Agreement contains a "Code of Conduct" that reads as follows in pertinent part:

> a. By agreeing to these Terms, you're agreeing that, when using the Services, you will follow these rules:
>
> i. Don't do anything illegal.
>
> ii. Don't engage in any activity that exploits, harms, or threatens to harm children.
>
> . . . .

> x. Don't help others break these rules.
>
> b. Enforcement. If you violate these Terms, we may stop providing Services to you or we may close your Microsoft account or Skype account. We may also block delivery of a communication (like email or instant message) to or from the Services in an effort to enforce these Terms or we may remove or refuse to publish Your Content for any reason. When investigating alleged violations of these Terms, Microsoft reserves the right to review Your Content in order to resolve the issue. However, we cannot monitor the entire Services and make no attempt to do so.

Id. at 840.

Before a Microsoft customer may create a Skype account, he or she must agree to the applicable terms of service, including the applicable Services Agreement. Exhibit 2, ¶ 4.

B. NCMEC

NCMEC is a private nonprofit corporation, incorporated under District of Columbia law, with a mission to help find missing children, reduce child sexual exploitation, and prevent child victimization. *See* Exhibit 3, Declaration of John Shehan, Vice President of the Exploited Children Division at NCMEC, ¶ 2. Like other large nonprofits, NCMEC receives federal grant and private foundation funding, corporate financial and in-kind donations, and private individual donations in support of its mission. *Id.* ¶¶ 3-4.

NCMEC also operates various programs in pursuit of its mission, among them the CyberTipline. The CyberTipline receives leads and tips regarding suspected crimes of sexual exploitation committed against children. In particular, it provides the public and ESPs a method of reporting internet-related child sexual exploitation, including child pornography offenses. NCMEC created a secure CyberTipline in February 2000 to facilitate the reporting of apparent child pornography by ESPs. ESPs register with NCMEC and can then upload files (*e.g.,* images and videos) relating to child sexual exploitation in connection with their report. *Id.* ¶¶ 5-6. NCMEC devised and implemented the CyberTipline with private funds and without any law

enforcement or government input. Indeed, the CyberTipline predates any federal legislation that references it. *Id.* ¶¶ 8-9; *see* 18 U.S.C. § 2258A.

NCMEC does not direct or mandate the type of information ESPs may choose to provide; instead, the CyberTipline contains voluntary reporting fields that ESPs may elect to populate with information, including uploading apparent child pornography files. NCMEC cannot alter or change information submitted by a reporting ESP. One voluntary field in Section A of the CyberTipline report is: "Was File Reviewed by the Company?" An ESP may choose to populate this field to indicate whether it reviewed an uploaded file prior to its submission to NCMEC. If the ESP provides the information, the field will populate with an affirmative or negative response; if it opts not to answer, the field will not appear in the CyberTipline report. Exhibit 3, ¶¶ 9-10.

Another voluntary reporting field contained in Sections A and B is: "Image Categorization by ESP." Image categorization is a result of a voluntary initiative of ESPs under which they categorize images based on the age of the victim and content depicted. If an ESP elects to furnish information related to categorization of an uploaded image, the field will automatically populate in Sections A and B of the CyberTipline report. If it opts not to populate the field, the field will not appear in the report. *Id.* ¶ 11.

After an ESP makes a CyberTipline report, a NCMEC staff member uses conventional and publicly-available open-source tools to attempt to identify potential geographic information pertaining to the individual who is the subject of the report, also relying on geographic information provided by the ESP in connection with the reported image. The results of these queries are contained in Section C of the CyberTipline report. *Id.* ¶¶ 13-14.

NCMEC is required to make CyberTipline reports available to law enforcement, but is not required to open a reported file or review any other content of a report. NCMEC staff members decide whether to open files pursuant to internal organizational and operational guidelines. In particular, NCMEC does not open or view every image file submitted in a CyberTipline report;[3] rather, the decision is driven by staff members' independent judgment, and informed by considerations such as volume of images reported, and considerations of child safety and imminent child endangerment. *Id.* ¶¶ 15-16. Once a staff member determines potential geographic location and completes report processing, she makes the report available to law enforcement in that region for potential investigation via NCMEC's secure virtual private network. *Id.* ¶ 17.

C. The Events Of This Case.

In May and June 2016, NCMEC received 44 CyberTips from Micrsoft/Skype, each tip containing only a single child pornography file shared through Skype instant messaging. In July and August, 2016, NCMEC received an additional 20 related CyberTips from Microsoft, each of these also containing a single child pornography file, as well as information provided by Microsoft pertaining to the screenname of the user who uploaded the file. *Id.* ¶¶ 18-93; Exhibit 2, ¶ 2.[4] As to each report/child pornography file, the reporting field "Was File Reviewed by the Company?" is answered "Yes." Exhibit 3, ¶¶ 18-93, Exhibit 2, ¶ 2. This fact is highlighted prominently in the publicly-filed documents in this case. The search warrant affidavit for

[3] As of June 10, 2017, NCMEC has received more than 21.2 million CyberTipline reports. Due to volume, it is not possible to review all reports, much less all images. *Id.* ¶ 16.

[4] The 64 CyberTipline reports are appended to Exhibit 2 (see attachment A). The original 44 tips were produced to the defense within two weeks of arraignment. Due to an apparent oversight, the remaining 20 tips were not produced until after the filing of the Motion to Suppress.

Coyne's residence and criminal complaint affidavit state: "the [child pornography] files were reviewed by Skype prior to reporting them to NCMEC." Exhibit 4, Complaint Affidavit, ¶ 15; Exhibit 5, Search Warrant Affidavit, ¶ 21.[5] Moreover, for each CyberTipline report, Microsoft populated the "Image Categorization by ESP" section with its description of age and content. Exhibit 3, ¶¶ 18-93; Exhibit 2, ¶ 2.[6] In this case, a NCMEC staff member elected to view each uploaded image. Exhibit 3, ¶¶ 18-93.

After conducting queries, NCMEC made the tips available to Homeland Security Investigations and the Vermont Office of the Attorney General for potential investigation. *Id.* 94-95. Detective Matthew Raymond, the Commander of the Vermont Internet Crimes Against Children Task Force identified the subscriber to the IP address (Richard Coyne) with a Bennington, Vermont address.[7] Investigation revealed that James Coyne (Richard's son), who was on federal supervised release for a child pornography conviction, resided at that address. On November 29, 2016, HSI Special Agent Caitlin Moynihan obtained a federal warrant to search

[5] Indeed, the exhibits to Coyne's Motion make this point with crystal clarity. *See* Defense Exhibit A. Defense Exhibit A contains two NCMEC CyberTipline reports related to this case, which are exemplary of the remaining 62. These reports contain the affirmative response in the field "Was File Reviewied by the Company?"

[6] In the two reports appended to Coyne's Motion, the ESP categorizations are "A1" and "A2." A1 means that the ESP determined that the reported file contained an image of a prepubescent minor and involved a "sex act,' defined as "[a]ny image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value." A2 means that the ESP determined that the reported file contained an image of a prepubescent minor and involved a "lascivious exhibition," defined as "any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value." *See* Defense Exhibit A

[7] Two of the sixty-four tips resolved to a separate IP address in Readsboro, a town located in Bennington County.

Coyne's Bennington residence. During that search, law enforcement observed Coyne in possession of a cell phone; subsequent search of that phone turned up as substantial amount of child pornography. Agents arrested Coyne for possession of child pornography. He is charged by Indictment with that offense. *See* Exhibits 4 and 5.

III. LEGAL FRAMEWORK

A. First Principles

The Fourth Amendment to the Constitution protects persons against unreasonable searches and seizures in their persons, houses, papers, and effects. U.S. Const. amend IV. "The basic purpose of this Amendment . . . is to safeguard privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Mun. Court of City & Cnty of S.F.*, 387 U.S. 523, 528 (1967). "The exclusionary rule has traditionally barred from trial physical, tangible materials obtained either during or as a direct result of an unlawful" search or seizure. *Wong Sun v. United States*, 371 U.S. 471, 485 (1963). Fourth Amendment protections attach when a "search" occurs – that is, when the government infringes on a reasonable expectation of privacy, *Katz v. United States*, 389 U.S. 347, 351 (1967), or where the government physically intrudes on a constitutionally-protected area for the purpose of obtaining information, *United States v. Jones*, 565 U.S. 400, 413 (2012).

The Fourth Amendment is wholly inapplicable "to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any government official." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (no "search" implicating the Fourth Amendment where DEA merely repeated the investigation of a package already conducted by a FedEx employee). Thus, "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Id.* at 117. As such, "even a wrongful

search . . . conducted by a private party does not violate the Fourth Amendment." *Walter v. United States*, 447 U.S. 649, 656 (1980). And, "such private wrongdoing does not deprive the government of the right to use evidence that it has lawfully acquired." *Id.*; *see also United States v. $557,933.89 in U.S. Funds*, 287 F.3d 66, 87 (2d Cir. 2002) ("As long as [the detective's] search of the briefcase was of no greater scope or intensity than the airport security personnel's, then 'no additional invasion of [claimant's] privacy interest' occurred and there was no additional 'search' for purposes of the Fourth Amendment.") (quoting *Arizona v. Hicks*, 480 U.S. 321, 325 (1987) and citing *Jacobsen*).

B. The *Ackerman* Case

On August 5, 2016 – several months after Microsoft made the original 44 CyberTipline reports in this case – the Tenth Circuit handed down *United States v. Ackerman*, 831 F.3d 1292 (10th Cir.). In *Ackerman*, the defendant sought suppression of evidence in a child pornography case that arose after AOL's automated hash value filter[8] identified as child pornography one of four images attached to an email he transmitted. After zeroing in on that one image, AOL stopped delivery of the email, shuttered the defendant's account, and forwarded the email – along with all four attachments – to NCMEC, where an analyst opened the email and viewed each of the four attached images (not just the one snared in the filter) and confirmed that they all appeared to be child pornography. NCMEC also identified the defendant as the likely owner of the account and alerted law enforcement agents in the area he lived. Federal charges ensued. The defendant sought suppression, claiming that NCMEC is a governmental agency or agent and

[8] AOL's filter relies on hash value matching. AOL's filter identifies the hash values of images attached to emails sent through mail servers. Those hash values are then compared to the hash values of images that AOL employees have previously viewed and deemed child pornography. An email containing an image with a matching value is automatically culled and forwarded to NCMEC's cybertip line. *Id.* at 1294.

its actions amounted to an unreasonable search of his email and attachments without a warrant or other lawful basis to search. *Id.* at 1294-95.

In an analysis summarized in detail in Coyne's Motion, the *Ackerman* Court concluded that NCMEC is a governmental entity, *id.* at 1301, or at minimum acted as a government agent, *id.* at 1303-04, and that NCMEC conducted a warrantless search of the defendant's "papers and effects" (that is, his email and all of its attachments) that exceeded the scope of the search (of only one attachment) conducted by AOL, *id.* at 1306-07. Noting that the government failed to raise the good faith exception (and potentially other viable arguments), the Court reversed the district court's denial of the Motion to Suppress and remanded for further proceedings, including a determination of whether the "third-party doctrine" might preclude the defendant's claim. *Id.* at 1304-05, 1308-09 ("it's an open question whether the Supreme Court's so-called 'third-party doctrine' might undermine any claim to Fourth Amendment protections when someone (like Mr. Ackerman) engages a *private agent* (like AOL) to deliver his correspondence.") (emphasis added).

In its decision, the Court also dealt with the government's invocation of the "private search" doctrine promulgated in *Jacobson*, 466 U.S. 109. Having already characterized AOL as a "private agent," the Court explained its view of the inapplicability of the private search doctrine to the facts of its case:

> Yes, AOL ran a search that suggested a hash value match between one attachment to Mr. Ackerman's email and an image AOL employees had previously identified as child pornography. But AOL never opened the email itself. Only NCMEC did that, and in at least this way, exceeded rather than repeated AOL's private search. Neither is there any doubt NCMEC's search of the email itself easily could have disclosed information previously unknown to the government besides whether the one attachment contained contraband . . . . And we know, too, that this particular container did contain three additional attachments, the content of which AOL and NCMEC knew nothing about before NCMEC opened them.

Id. at 1305-07 (also questioning the status of *Jacobson* after *Jones*, which held that government conduct can constitute a Fourth Amendment search either when it infringes on a reasonable expectation of privacy or when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing for purposes of obtaining information).

In conclusion, the *Ackerman* Court acknowledged the possibility that "changes in how reports are submitted or reviewed might allow NCMEC to access attachments with matching hash values directly, without reviewing email correspondence with possibly private, noncontraband content – and in this way perhaps bring the government closer to a successful invocation of the private search doctrine." *Id.* at 1308-09 (Further recognizing "it may be possible that the government could cite exigent circumstances or attenuation doctrine or special needs doctrine or the good faith exception to excuse warrantless searches or avoid suppression in at least some cases").

C. ESPs Act as *Private Entities* When Monitoring User Activities on their Services.

Ackerman labeled AOL a "private agent," but it did not squarely address the question whether ESPs act as government agents when they monitor user activities on their servers. The Circuits to address the issue uniformly reject the "ESP-as-government-agent" theory. *See United States v. Cameron*, 699 F.3d 621, 638 (1st Cir. 2012) ("[I]f Yahoo! Chose to implement a policy of searching for child pornography, it presumably did so for its own interests"; observing that fact that child pornography is a government interest does not mean that an ESP "cannot voluntarily choose to have the same interest"); *United States v. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013) ("AOL's decision on its own initiative to ferret out child pornography does not convert the company into an agent or instrument of the government for Fourth Amendment purposes . . . . AOL's voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent."); *United States v.*

Richardson, 607 F.3d 357, 366 (4th Cir. 2010) (holding that AOL's scanning of email communications for child pornography did not trigger the Fourth Amendment's warrant requirement because no law enforcement officer or agency asked the provider to search or scan the defendant's emails).

Lower courts have, without exception, followed suit. *E.g.*, *United States v. Stratton*, 2017 WL 169041, No. 15-40084-01-DDC (D. Kan. January 17, 2017) (discussed below); *United States v. Drivdahl*, No. CR 12-18-H-DLC, 2014 WL 896734, at *3-4 (D. Mont. Mar. 6, 2014) (finding there was "simply nothing in the record to suggest that law enforcement agents were involved in the search or investigation of [defendant's] activities" and that "the suspect material was opened by a Google employee prior to being turned over to the government [t]hus, there was no expansion of the private search"); *United States v. Lien*, 16-cr-00393-RS-1, at *7 (N.D. Cal. May 10, 2017) (denying Motion to Suppress, "Google opened and viewed the uploaded images files prior to submitting its Cybertip. NCMEC then opened and viewed the exact same image files. NCMEC's search thus did not exceed the scope of the private search"); *United States v. Miller*, 16-47-ART-CJS (E.D. Ky. (May 19, 2017) (defendant challenged Google's search of his email account for child pornography using hashing technology, alleging ISP was government actor with statutory requirements to report to NCMEC; noting defense counsel cited no authority for the proposition and holding that "Google's actions in this case were motivated by business interests" and "there is no evidence or allegation that Google sent anything to NCMEC other than the files of the two images having a hash value match to two images Google's employees had previously identified as being apparent child pornography."); *United States v. Keith*, 980 F. Supp. 2d 33, 44 (D. Mass. 2013) (finding AOL, motivated by its own wholly private interests in monitoring emails for child pornography, was not acting as a government agent in searching its

network for child pornography and reporting any findings to NCMEC); *United States v. Green*, 857 F. Supp. 2d 1015, 1019 (S.D. Cal. 2012) (same); *United States v. DiTomasso*, 81 F. Supp. 3d 304, 309 (S.D.N.Y. 2015) (chat service provider not a government agent and its search of defendant's chat messages held to be a purely private search beyond the reach of the Fourth Amendment); *United States v. Wilson*, 3:15-cr-2838-GPC, 14-20 (S.D. Cal. June 26, 2017) (concluding that Google conducted a private search of the contents of defendant's email and law enforcement did not significantly expand that search).

Indeed, in the wake of *Ackerman*, a district court in the Tenth Circuit rejected a child pornography defendant's claim, grounded on *Ackerman*, that ESP Sony acted as a government agent when it intercepted electronic images, attachments, and image downloads and forwarded them to NCMEC. *Stratton*, 2017 WL 169041. "*Ackerman*," the Court observed, "discusses the comprehensive statutory structure governing NCMEC." *Id.* at 5 (summarizing *Ackerman's* recitation of the various congressional mandates concerning NCMEC collaboration with law enforcement). Contrasting the statutory regimes applicable to NCMEC and ESPs, the Court explained:

> The only similar statute governing Sony is 18 U.S.C. § 2258. And § 2258 only requires Sony to file a report if it learns of facts that suggest an incident of child abuse. Unlike the statute government NCMEC, § 2258 does not require Sony to act affirmatively to monitor its users' accounts, review its users' downloads, or maintain any sort of reporting system for abuse of Sony's PSN. Sony monitors its users' accounts to protect its own interests in a safe online gambling community. Nothing . . . suggests that Sony consented to act on behalf of the government or subject to its control.

Id. Concluding that the ESP did not act as a government agent, the Court further held that NCMEC did not exceed the scope of the ESP's private search. It specifically held that the facts differed from *Ackerman* because Sony viewed all files in question, whereas, in *Ackerman*, "the undisputed facts established that NCMEC opened and viewed information other than the image

that was the target of AOL's hash value match and 'that AOL had not previously examined.'" *Id.* at 7. Accordingly, the Fourth Amendment was not implicated. *Id.* at 6-8 (citing *Jacobsen* for the proposition that, "if results of the private search are turned over to the government, the government may not exceed the scope of the private search unless it has a right to conduct an independent search") (internal quotations omitted).

In any event, the Court observed, even if a Fourth Amendment violation occurred, the good faith doctrine salvaged the fruits of the ensuing residence search warrant because the affiant "had no reason to believe that Sony had provided NCMEC with information procured in violation of defendant's Fourth Amendment rights." Indeed, "there was no evidence NCMEC had exceeded the scope of its authority when it relied on the information Sony provided" and "when the officers executed the search warrant on defendant's home, they had no reason to believe the warrant was obtained in violation of defendant's Fourth Amendment rights." *Id.* at 9 (further holding that the case did not fall within any of the four exceptions to the good faith doctrine).

IV. ARGUMENT

A. *Ackerman* Was Wrongly Decided And Inconsistent With Second Circuit Precedent.

The thrust of Coyne's Motion is an 8-page *Ackerman*-based argument that NCMEC is a government entity. This argument, of course, presupposes that *Ackerman* was correctly decided. It was not. On the contrary, *Ackerman's* holding that NCMEC is a government entity reflects a misapplication of controlling Supreme Court precedent. It is also contrary to Second Circuit case law.

The *Ackerman* panel relied heavily on *Lebron v. Nat'l R.R. Passenger Corp.*, 513 U.S. 374, 399 (1995), to "fortify [its] conviction that NCMEC qualifies as a governmental entity."

831 F.3d at 1297. In *Lebron*, the Court held that a corporation is a government entity subject to constitutional constraints where "the government creates a corporation by special law, for the furtherance of governmental objectives, and retains for itself permanent authority to appoint a majority of the directors of that corporation." 513 U.S. at 400; *see also Dep't of Transp. v. Ass'n of Am R.Rs.*, 135 S. Ct. 1225, 1227 (2015) ("*DOT*") (reciting the same operative factors, noting that "federal control and supervision" are necessary attributes of a government entity).

NCMEC simply does not qualify. It is, in fact, a privately incorporated entity, not a statutorily created one. Exhibit 3, ¶ 2. The *Ackerman* panel found that various statutory requirements "evince[] a sort of 'day-to-day' statutory control over [NCMEC's] operations that the Court found tellingly present in the Amtrak cases." *Id.* at 1298. But this misconstrues the reasoning of *Lebron* and *DOT*, which turned on the fact that the federal government "retains for itself permanent authority to appoint a majority of the directors" of the company. *Lebron*, 513 U.S. at 398-99 (noting this circumstance meant that Amtrak operated "under the direction and control of federal governmental appointees"); *DOT*, 135 S.Ct. at 1233 (emphasizing "the practical reality of federal control and supervision"). The same is not true of NCMEC. The government does not choose the majority of its board of directors or retain the authority to do so. *See Ackerman*, 831 F.3d at 1298 & n.5 (recognizing that, at most, "a quarter of NCMEC's board members represent government agencies and law enforcement"); *Lazaridis v. U.S. Dep't. of Justice*, 713 F. Supp. 2d 64, 68 (D.D.C. 2010) (observing NCMEC's "website [does not] suggest[] that the executive branch has a hand in appointing board members"); Exhibit 6, NCMEC *Ackerman* Amicus Brief, Addendum (NCMEC articles of incorporation).[9] Not

[9] In opposing Coyne's claim that NCMEC is a government entity/agent, the government relies on, and incorporates, the in-depth arguments advanced in the Amicus Brief for NCMEC filed in

surprisingly, therefore, the First Circuit, having considered the relevant statutory scheme – including NCMEC's federal funding – held that the organization is "not officially a government entity." *Cameron*, 699 F.3d at 644; *see also United States v. Orleans*, 425 U.S. 807, 815-16 (1976) ("The Federal Government in no sense controls the detailed physical performance of all the programs and projects in finances by gifts, grants, contracts, or loans.") (citation and internal quotation omitted); Exhibit 7, at 14 (cataloguing examples of entities that receive federal funds and experience government oversight but are nonetheless not regarded as components of the government).

This Court should reach the same conclusion. Indeed, that result is the only one that can be reconciled with Second Circuit precedent. *See Hack v. President and Fellows of Yale College*, 237 F.3d 81, 83-84 (2d Cir. 2000). In *Hack*, the Court considered whether Yale qualified as a government entity within the meaning of *Lebron*. It acknowledged that the state created the entity by special law, thus satisfying part of the *Lebron* standard – while also clarifying that this circumstance is a prerequisite to treating an entity as an arm of the government. The plaintiff claimed that it would be overly simplistic to read *Lebron* as strictly requiring "majority government control." It urged the Court to find that, even though only two of Yale's nineteen board members came from government, they had outsized influence and wielded enough government control to satisfy the *Lebron* standard. The Second Circuit disagreed, explaining:

> We think *Lebron* means what it says. Indeed, the Court there contrasted Comsat with Amtrak, noting that the President appointed only three of fifteen Comsat directors, 513 U.S. at 391, 115 S.Ct. 961, and describing it as a private corporation not government-controlled, *id.* at 397, 115 S.Ct. 961. Moreover, the Court has indicated its reluctance to have the federal courts indulge in evaluations of the effectiveness of governmental

---

Ackerman (with its addendum), Exhibit 6, and on the United States' brief in support of Petition for Panel Rehearing in *Ackerman*, Exhibit 7. The government's Petition was denied.

> persuasion, absent government control. *See San Francisco Arts & Athletics, Inc. v. United States Olympic Comm.*, 483 U.S. 522, 545–546 n. 27, 107 S.Ct. 2971, 97 L.Ed.2d 427 (1987). Plaintiffs do not suggest that Connecticut had any involvement in establishing Yale's parietal rules. It is equally clear that the state could not control Yale's policies and operations even if it chose to become involved. Yale, as a private university, did not act under color of law.

237 F.3d at 83-84; *see also Sprauve v. W. Indian Co.*, 799 F.3d 226, 233 (3d Cir. 2015) (also finding that *Lebron* does not apply unless the government created the entity by statute).

In reaching its conclusion, *Ackerman* stretched the *Lebron* holding to a result inconsistent with its plain language. By contrast, the Second Circuit has decided that the opinion "mean[s] what it says" – and it says that an entity is not a government component unless it is created, and majority-controlled, by the government. NCMEC being neither, this Court should find that the organization is a private entity under controlling Supreme Court and Second Circuit precedent.

B. There Was No "Search" Within The Meaning Of The Fourth Amendment.

i. The Fourth Amendment Does Not Apply Because Microsoft, A Private Entity, Examined All Files In Question Before Transmitting Them To NCMEC.

In any event, the government entity question is an academic one: even if Coyne is right about NCMEC, there was no "search" within the meaning of the Fourth Amendment because Microsoft, a private party, reviewed each contraband image in question prior to transmitting it to NCMEC. Coyne either overlooks or ignores this Motion-dispositive fact.

Here, as in cases like *Stratton*, *Miller*, and *Lien*, Microsoft, a private party, viewed and categorized each contraband image, indicating its findings by populating the relevant fields within the NCMEC CyberTipline reports. This circumstance takes the case out of the *Ackerman* paradigm, as the opinion itself recognizes. 831 F.3d at 1308-09 ("changes in how reports are submitted or reviewed might allow NCMEC to access attachments with matching hash values directly, without reviewing email correspondence with possibly private, noncontraband content – and in this way perhaps bring the government closer to a successful invocation of the private

search doctrine."). NCMEC's review of each file at issue, did not exceed that of Microsoft's in "scope or intensity." The NCMEC examination did not reveal – and did not have the potential to reveal – any additional information. Under these circumstances, the Fourth Amendment is inapplicable. *Jacobson*, 466 U.S. at 109.[10]

While Coyne ignores or obscures the private search doctrine, he nonetheless seems to anticipate its significance without mentioning it directly – that is, he asserts, in conclusory fashion, that "Microsoft/Skype act as governmental agents when they actively monitor their networks . . . for contraband based on parameters provided by the government." Motion at 12-13. In support of this assertion, he cites generic case law concerning agency relationship and regurgitates his *Ackerman*-based NCMEC-as-government-agent theory. *Id.* at 12 ("For essentially the same reasons . . . . "). His argument is specious. To begin, Microsoft does not monitor its networks "based on parameters provided by the government," but rather, using technology it developed working with another private party and in furtherance of its own myriad business interests. But, more importantly, Coyne's pages-long argument that Microsoft is a government agent does not even attempt to grapple with the body of on-point case law from

[10] The government is advised by Microsoft outside counsel that Microsoft technicians performing manual review of child pornography images do not typically see the associated username, only the image. As to the 20 tips submitted in July and August 2016, Microsoft furnished the screenname of the user who uploaded each child pornography image. The original 44 tips had no associated username, only an image. Even assuming that (1) Microsoft employees did not review the screennames for the last 20 tips (which seems unlikely because Microsoft provided the screenname information to NCMEC along with the contraband image); (2) NCMEC is a government entity/agent (a point the government does not concede); and (3) NCMEC somehow exceeded the scope of Microsoft's review by seeing the screenname it provided, suppression is unwarranted. The original 44 CyberTipline reports contained only uploaded files, which Microsoft indisputably reviewed. Those reports provide an independent source of probable cause for the Coyne residence search warrant. *Murray v. United States*, 487 U.S. 533 (1988) (probable cause from source independent of illegality may support the warrant).

across the country, all of which holds just the opposite: that ESPs behave as private entities when they monitor user accounts for criminality.

The result should be no different here. Like ESPs in similar cases, Microsoft's "independent business judgement" caused it to develop and deploy PhotoDNA to intercept images of child sexual abuse. The monitoring scheme fosters a better and safer online atmosphere and improves Microsoft's image and reputation. No government agent directed, or even asked, Microsoft to use the technology. If Microsoft discovers criminality – through its own initiative and privately-developed monitoring technology – only then does it comply with the legal requirement to forward the contraband to NCMEC. But none of Microsoft's efforts to root out criminality within its services arises from government requirements or even government suggestions. Coyne's claim otherwise is wholly unmoored to authority and should be rejected.

ii. The "Trespass" Theory of Search Articulated In *Jones* Does Not Change The Analysis.

In *Ackerman*, the Court wondered, *in dicta*, whether, the private party doctrine articulated *Jacobsen* survived *Jones*. 831 F.3d at 1307-08 ("Reexamining the facts of *Jacobsen* in light of *Jones*, it seems at least possible the [Supreme] Court today would find that a "search" did take place there. After all, the DEA agent who performed the drug test in *Jacobsen* took and destroyed a 'trace amount of property, a seeming trespass."). *Jacobsen* invoked the "reasonable expectation of privacy standard" in deciding whether a search had occurred. *See Katz,* 466 U.S. at 122-23. *Jones*, however, held that that formula is but one way to determine if a constitutionally qualifying search occurred. After *Jones*, government conduct can constitute a Fourth Amendment search *either* when it infringes a reasonable expectation of privacy *or* when it involves a physical intrusion (a trespass) on a constitutionally protected space for purposes of obtaining information. *Jones*, 565 U.S. at 413. The *Ackerman* Court opined, again in *dicta*, that

NCMEC's warrantless opening and examination of private correspondence "seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent." *Id.* at 1307.

For his part, Coyne makes a cursory argument that NCMEC's actions amounted to a "search" within the meaning of *Jones* (and *Katz*), Motion at 13-14, but, in so doing, he continues to steer clear of *Jacobsen* and the private search doctrine. In any event, the question arises: even if NCMEC's search did not infringe a reasonable expectation of privacy (because of the earlier private search of the same scope), did it nonetheless involve a trespass that contravened the Fourth Amendment?

Jones involved installation of a GPS tracker on a suspect's car and the subsequent tracking of vehicle location. 565 U.S. at 404. *Jones* expressly declined to predict its effect on "some future case where a classic trespassory search is not involved." *Id.* at 412 (emphasis added). In particular, it noted that "[s]ituatons involving merely the transmission of electronic signals without trespass would remain subject to the *Katz* analysis," *id.* at 411, and that resort to *Katz* analysis would generally be necessary absent a classic trespassory search. *Id.* at 412. The courts to consider the issue – whether NCMEC "trespasses" when it looks at files already reviewed by an ESP – have answered in the negative. *See Lien*, 3:16-cr-393, at 7-8 (finding *Ackerman's* discussion of *Jones* unpersuasive); *Miller*, 2:16-cr-47, at 26 n. 10 ("*Jones* did not involve the application of the private search doctrine, and *Ackerman* involved a finding that the Government exceeded the scope of AOL's private search"). Courts have also deemed *Jones* inapplicable in analogous contexts. *See United States v. Bode*, No. CRIM. ELH-12-158, 2013 WL 4501303, at 9 n.16 (D. Md. Aug. 21, 2013) (finding *Jones* inapplicable to a case involving child pornography charges stemming from government investigation of postings in a chatroom);

United States v. Wheelock, No. 13-CR-136, 2013 WL 12074960, at *5 (D. Minn. Sept. 12, 2013), *report and recommendation adopted*, 2013 WL 12074962 (D. Minn. Oct. 17, 2013), *aff'd*, 772 F.3d 825 (8th Cir. 2014) (finding *Jones* inapplicable in a case involving child pornography charges based on government investigation of IP address). This Court should reach the same conclusion.

In sum, because no government agent or entity conducted a search, the Fourth Amendment is inapplicable and the Court should deny Coyne's Motion.

C. Coyne Had No Reasonable Expectation Of Privacy In His Skype Instant Messages.

Even if the Court finds that a search by a government entity/agent occurred, it should nonetheless deny the Motion because Coyne had no reasonable expectation of privacy in his Skype messages. A search, for purposes of the Fourth Amendment, occurs if there is "actual intrusion into a constitutionally protected area." *Kyllo v. United States*, 533 U.S. 27, 231 (2001). An area is constitutionally protected only if "the individual manifested a subjective expectation of privacy in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable." *Id.* at 233; *see also United States v. Hagg*, 278 F.3d 44, 47 (2d Cir. 2002).

In *Ackerman*, the Court recognized that "it's an open question whether the Supreme Court's so-called 'third-party doctrine' might undermine any claim to Fourth Amendment protections when someone (like Mr. Ackerman) engages a private agent (like AOL) to deliver his correspondence." 831 F.3d at 1304 (citing *United States v. Miller*, 425 U.S. 435, 440-43 (1976) and *Smith v. Maryland*, 442 U.S. 735, 742-46 (1979), which hold that individuals lack any reasonable expectation of privacy and so forfeit any Fourth Amendment protections in materials they choose to share with third parties like banks or phone companies). The Court thus

remanded to the district court for "factual findings relevant to Mr. Ackerman's subjective expectations of privacy or the objective reasonableness of those expectations in light of the parties' dealings (*e.g.*, the extent to which AOL regularly accessed emails and the extent to which users were aware of or acquiesced in such access)." *Id.* at 1305.

The weight of authority appears to hold that, as a *general matter*, users of online messaging services are entitled to a reasonable expectation of privacy in their use of those services and thus at least *eligible* for Fourth Amendment protection. *See, e.g.*, *United States v. Hamilton*, 701 F.3d 404 (4th Cir. 2012) (stating, in the marital privilege context, that "email has become the modern stenographer . . . . emails today, in common experience, are confidential") (quotation and citation omitted); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding "that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial [internet service provider]") (quotations omitted); *United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) (same); *but see United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2007) (finding no Fourth Amendment protection for the to/from addresses of email messages).

This precedent, however, also recognizes that a subscriber agreement might "snuff out" the reasonable expectation of privacy in online communications. *See, e.g.*, *Warshak*, 631 F.3d at 286-87 (finding that the mere *ability* or *right* of the ISP to access emails was insufficient to extinguish the expectation); *Hamilton*, 701 F.3d at 408-09 (computer usage policy acknowledged by defendant put him "on notice" of company oversight and defeated his expectation). Other courts have dealt with the question of diminished expectation of privacy in slightly different contexts. *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000), for example, involved a government employee prosecuted for child pornography offenses after his employer-agency

discovered contraband files on his government-issue computer. The agency maintained an internet usage policy that, among other things, prohibited accessing unlawful material and warned that the agency conducted electronic audits of usage to identify and prosecute unauthorized activity. One of these audits uncovered child pornography on the defendant's computer. In affirming the denial of the defendant's motion to suppress, the Fourth Circuit stated that government employees may have a legitimate expectation of privacy, but it can be diminished by office practices, procedures, or regulations. It held that the defendant lacked a legitimate expectation of privacy in files downloaded from the internet because office policy put him "on notice that [he] could not reasonably expect [his] internet activity would be private." *Id.* at 396; *see also United States v. Angevine*, 281 F.3d 1130, 1132-35 (10th Cir. 2002) (defendant lacked legitimate expectation of privacy in data downloaded from internet on university computers because university policy reserved the right to audit and warned that legal action could result from internet use in violation of federal law); *cf. United States v Caraballo*, 963 F. Supp. 2d 341, 363 (D. Vt. 2013) (Reiss, C.J.) (concluding that the defendant lacked a subjective expectation of privacy in his phone given the terms of Sprint's service agreement, and that, in any event, such an expectation is not one society is prepared to accept as reasonable), *affirmed on other grounds*, 830 F.2d 19, (2d Cir. 2016).

Here, there is no question that, before Coyne created his Skype account, he agreed to the applicable Services Agreement. Exhibit 2, ¶ 4. By agreeing to its terms, he extinguished any reasonable expectation of privacy he had in the activity on his account. The Services Agreement advised him that, "By . . . agreeing to these Terms, you consent to Microsoft's collection, use and disclosure of Your Content and Data as described in the Privacy Statement." It further stated, in no uncertain terms: "we collect content of your files and communications . . . ." *Id.*,

Attachment B. It further explained: "we will access, transfer, disclose, and preserve personal data, including your content . . . . when we have a good faith belief that doing so is necessary to . . . comply with applicable law or respond to valid legal process . . . ." By agreeing to the Services Agreement, Coyne also agreed to follow the "Code of Conduct," which included the admonitions, "don't do anything illegal"; "don't engage in any activity that exploits, harms, or threatens to harm children"; and "don't help others break these rules." Finally, in signing up for his Skype account, Coyne was warned: "If you violate these Terms, we may stop providing Services to you or we may close your Microsoft account or Skype account. We may also block delivery of a communication (like an email or instant message) in an effort to enforce these Terms . . . . When investigating alleged violations . . . Microsoft reserves the right to review Your Content in order to resolve the issue." *Id.*

In short, Coyne was "on notice" that he could not reasonably expect privacy on his Skype account – particularly not as it related to child exploitation activity on that account. *See Hamilton*, 701 F.3d at 408-09; *Simons*, 206 F.3d at 396. This is not a case in which the subscriber agreement merely alluded to the ESP's "ability" to monitor online activity, *compare Warshak*, 631 F.3d at 286-87, but rather, an instance in which the agreement unequivocally warned Coyne that the company would affirmatively "collect" and "access" his communications in order to enforce its Code of Conduct, protect children, and comply with the law. Through his agreement to these terms, Coyne "snuffed out" his expectation of privacy and, with it, any claim of Fourth Amendment violation. *See Wilson*, 3:15-cr-2838, at 13 (finding that the defendant's agreement to an "express [Google] monitoring policy regarding illegal content . . . rendered [his] subjective expectation of privacy in the four uploaded child pornography attachments objectively unreasonable," but ultimately resting decision on other grounds) (citing *Simons*, 206 F.3d at 398,

and *Angevine*, 281 F.3d at 1134); *Stratton*, 2017 WL 169041, at 7-9 (defendant lacked a reasonable expectation of privacy in downloaded images because he agreed to Sony Terms of Service).

D. The Good Faith Exception Applies.

Even if a Fourth Amendment violation occurred – because NCMEC and/or Microsoft acted as government entities/agents or NCMEC somehow exceeded the scope of Microsoft's private search or otherwise conducted an unlawful "search" – the good faith exception to the Fourth Amendment's exclusionary rule applies. *See United States v. Leon*, 468 U.S. 897 (1984). In *Leon*, the Supreme Court explained that, "[i]f the purpose of the [Fourth Amendment's] exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Id.* at 919. In other words, the exclusionary rule serves to deter "deliberate, reckless, or grossly negligent conduct." *Herring v. United States*, 555 U.S. 134, 144 (2009). Accordingly, to trigger the exclusionary rule, "police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.*

Here, there is not a scintilla of evidence that SA Moynihan, who acquired the warrant to search Coyne's residence, engaged in deliberate, reckless, or grossly negligent conduct. Put another way, there is no conduct to deter. When SA Moynihan wrote the warrant affidavit, she had no reason to suspect – let alone believe – that Microsoft and NCMEC procured information in violation of Coyne's Fourth Amendment rights. And why would she? Every case to address the issue has held that ESPs are private actors and that the Fourth Amendment is inapplicable when a NCMEC search merely replicates the scope of the ESP's. *See* Exhibit 5, ¶ 21; *Davis v.*

United States, 564 U.S. 229, 241 (2011) (applying good faith exception where agents acted in reasonable reliance on existing law later overturned); *Illinois v. Krull*, 480 U.S. 340, 356-57 (1987) (same). Indeed, given that only one out-of-circuit case decided in the midst of this investigation holds (contrary to Supreme Court and Second Circuit precedent) that NCMEC is a government entity/agent, SA Moynihan would not have been sufficiently culpable even if NCMEC's examination *had* somehow exceeded Microsoft's search (which it did not). The case law is far from settled on this score. *See e.g.*, *Stratton*, 2017 WL 169041, at *9-10 (deeming the good faith doctrine applicable for similar reasons). Moreover, SA Moynihan obtained a federal warrant, which gives rise to a presumption that she acted in good faith. *See Leon*, 468 U.S. at 922.

Of course, *Leon* envisioned four scenarios in which the exclusionary rule will apply even if the affiant secures a warrant. The first two involve circumstances where the judge issuing the warrant relies on a deliberately or recklessly false affidavit or otherwise abandons her judicial role and fails to perform the neutral, detached function. *Id.* at 914. There is no allegation, much less evidence, that that happened here.

The third *Leon* exception involves an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely questionable." *Id.* at 923. SA Moynihan's 16-page search warrant affidavit does not fit the bill. It outlines (1) the information Microsoft uncovered about a Skype user sharing a substantial number of child pornography files; (2) NCMEC's processing of the related 64 CyberTipline reports and its sharing of those reports with Vermont law enforcement; and (3) Vermont investigators' discovery that the IP address for 62 of the 64 reports resolved to the home of an individual (Coyne) on federal supervised release for a child pornography possession conviction. Under these circumstances, there can be no colorable

claim that SA Moynihan's affidavit suffered from a deficiency that would bring it within the third *Leon* carve-out, *see Stratton*, 2017 WL 169041, at *9-10, nor has Coyne, for that matter, attempted to mount such a claim.

Lastly, *Leon* describes an exception for warrants "so facially deficient" as to fail to particularize the place to be searched and things to be seized. *Leon*, 468 U.S. at 923. Again, there is no such shortcoming with this warrant. Coyne does not contend otherwise.

Coyne's only effort to overcome the good faith exception comes in a single sentence: "Nothing in *Leon* suggests that the rule should apply where there was no warrant and where there is no statute or law authorizing the warrantless search." Motion at 16-17. This tautology – made without citation to any authority – is, as a threshold matter, peculiar, because there was a federal warrant in this case, which turned up a sizeable stash of child pornography on Coyne's cell phone. It is also conflates the question of a Fourth Amendment violation with the question of good faith, when, in fact, the analyses are separate and distinct. In any event, Microsoft, a private entity, conducted the investigation that gave rise to the warrant, and NCMEC did no more than replicate the steps taken by Microsoft. Thus, Coyne cannot avoid application of the good faith doctrine. *See Stratton*, 2017 WL 169041, at 10 (rejecting defendant's attempt to avoid the good faith doctrine on similar grounds).

V. CONCLUSION

For the foregoing reasons, the government respectfully urges the Court to deny Coyne's Motion.

Dated at Burlington, in the District of Vermont, June 30, 2017.

Respectfully submitted,

UNITED STATES OF AMERICA

EUGENIA A.P. COWLES
Acting United States Attorney

By: */s/ Christina E. Nolan*
CHRISTINA E. NOLAN
Assistant U.S. Attorney
P.O. Box 570
Burlington, VT 05402-0570
(802) 951-6725
Christina.Nolan@usdoj.gov

CERTIFICATE OF SERVICE

I, Liza G. LaBombard, Legal Assistant for the United States Attorney for the District of Vermont, do hereby certify that on June 30, 2017, I electronically filed the Government's **OPPOSITION TO MOTION TO SUPPRESS EVIDENCE AND STATEMENTS** with the Clerk of the Court using the CM/ECF system.

/s /Liza G. LaBombard
Legal Assistant
District of Vermont
P.O. Box 570
Burlington, VT 05402
(802) 951-6725